Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje 2024

Kansallinen turvallisuusviranomainen

Ulkoministeriö
Utrikesministeriet

Sisältö

1 JOHDANTO

Tämän ohjeen tarkoituksena on selostaa ja kuvata kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseen kuuluvan turvallisuusluokitellun tiedon käsittelyyn liittyviä velvollisuuksia. Suomi on sitoutunut valtiosopimuksissa toteuttamaan tietoturvallisuustoimia sellaisen sopimusosapuolen turvallisuusluokitellun tiedon suojaamiseksi, joka on sopimuksen mukaisesti luovutettu Suomeen. Näiden velvoitteiden yleiseksi toteuttamiseksi on säädetty laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004).

Kansainvälisten turvallisuusluokiteltujen tietoaineistojen käsittelyyn sovelletaan viranomaisten toiminnan julkisuudesta annetun lain (621/1999; jäljempänä julkisuuslaki) yleisiä hyvää tiedonhallintatapaa koskevia velvoitteita sekä julkisen hallinnon tiedonhallinnasta annetun lain (906/2019; jäljempänä tiedonhallintalaki) yleisiä tiedonhallinnan järjestämistä koskevia velvoitteita, jollei kansainvälisistä tietoturvallisuusvelvoitteista annetusta laista muuta johdu. Näiden lisäksi käsittelyyn sovelletaan asiakirjojen turvallisuusluokittelusta valtionhallinnossa annettua asetusta (1101/2019; jäljempänä turvallisuusluokitteluasetus), jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu.

Tämä ohje ei korvaa sopimusmääräyksiä tai muita kansainvälisiä tietoturvallisuusvelvoitteita. Niiden, jotka tarvitsevat yksityiskohtaista tietoa velvoitteista, tulee käyttää ensisijaisena lähteenä kansainvälisiä tietoturvallisuusvelvoitteita määritteleviä säännöksiä ja sopimuksia.

Ulkoministeriö toimii kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa kansallisena turvallisuusviranomaisena (*National Security Authority*, NSA). Kansallisen turvallisuusviranomaisen lisäksi kansainvälisiä tietoturvallisuusvelvoitteita toteuttavina määrättyinä turvallisuusviranomaisina (*Designated Security Authority*, DSA) toimivat puolustusministeriö, Pääesikunta ja suojelupoliisi. Lisäksi Liikenne- ja viestintävirasto toimii kansallisena tietojärjestelmien ja tietoliikenteen tietoturvallisuudesta vastaavana viranomaisena (*National Communication Security Authority*, NCSA). Näillä kaikilla on omat vastuualueensa kansallisen turvallisuusviranomaisen tehtäväkentässä.

Tarvittaessa tapauskohtaista neuvoa ja ohjausta on syytä kääntyä kansallisen turvallisuusviranomaisorganisaation puoleen. Yleiset kysymykset osoitetaan ulkoministeriössä toimivalle kansalliselle turvallisuusviranomaiselle (nsa@gov.fi) ja sähköiseen tiedonsiirtoon liittyvät erityiskysymykset Liikenne- ja viestintäviraston NCSA-FI-yksikölle (ncsa@traficom.fi).

2 KANSAINVÄLINEN TURVALLISUUSLUOKITELTU TIETOAINEISTO

Kansainvälisellä turvallisuusluokitellulla tietoaineistolla tarkoitetaan kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitettua *erityissuojattavaa tietoaineistoa,* jota Suomen on kansainvälisen sopimuksen taikka Euroopan unionin (EU), Pohjois-Atlantin liiton (Nato) tai muun kansainvälisen järjestön turvallisuussääntöjen perusteella suojattava. Kansainvälisiä turvallisuusluokiteltuja tietoaineistoja ovat siten Suomeen toimitetut asiakirjat, aineistot, materiaalit ja näihin sisältyvät tiedot, joihin luovuttaja on tehnyt turvallisuusluokittelumerkinnän kansainvälisen tietoturvallisuusvelvoitteen mukaisesti. Niitä ovat myös Suomen esimerkiksi Natolle tai EU:lle luovuttamat turvallisuusluokitellut tietoaineistot silloin, kun aineisto liittyy kansainväliseen yhteistyöhön ja siihen on tehty EU:n tai Naton turvallisuusluokittelumerkintä.

2.1 Tietoaineiston salassapitovelvollisuus

Kansainväliseen turvallisuusluokiteltuun aineistoon sovelletaan kansainvälisistä tietoturvallisuusvelvoitteista annetun lain erityissäännöstä ehdottomasta salassapitovelvollisuudesta. Siihen ei kohdistu julkisuuslain mukaista salassapidon tapauskohtaista arviointia, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. Kansainväliset turvallisuusluokitellut tietoaineistot on siten pidettävä salassa, jollei niitä koskevista sopimuksista tai säännöistä muuta johdu.

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa on rangaistussäännökset salassapitovelvollisuuden rikkomisesta. Rangaistus salassapitovelvollisuuden, vaitiolovelvollisuuden ja hyväksikäyttökiellon rikkomisesta tuomitaan rikoslain (39/1889) mukaan joko virkasalaisuuden rikkomisena tai tuottamuksellisena virkasalaisuuden rikkomisena, salassapitorikoksena tai salassapitorikkomuksena, jollei siitä muualla laissa säädetä ankarampaa rangaistusta.

Kansallisen turvallisuusviranomaisen on ilmoitettava kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitetuissa tapauksissa toiselle sopimuspuolelle tietoonsa tulleesta turvallisuusluokiteltujen tietojen suojan vaarantumisesta ja tietoturvallisuutta koskevan määräyksen loukkaamisesta sekä ryhdyttävä toimenpiteisiin asian selvittämiseksi samoin kuin rangaistavaan tekoon syyllistyneen syytteeseen saattamiseksi.

2.2 Turvallisuusluokitellun tiedon suojaamisesta ja vaihtamisesta sopiminen

Turvallisuusluokitellun tiedon suojaamisesta sopiminen Suomen ja vieraan valtion taikka Suomen ja kansainvälisen järjestön välillä edellyttää valtiosopimusta. Tietoturvallisuussopimuksissa velvoitetaan sopimuspuolet huolehtimaan, että toisen sopimuspuolen turvallisuusluokiteltua tietoa käsitellään asianmukaisesti.

Suomen ja vieraiden valtioiden välisten tietoturvallisuussopimusten valmistelusta vastaa ulkoministeriössä toimiva NSA, ja valmisteluun osallistuvat ne hallinnonalat, joiden asiantuntemusta pidetään kulloinkin tarpeellisena.

2.3 Velvoitteet koskevat viranomaisia ja yrityksiä

Kansainvälisiä turvallisuusluokiteltuja tietoaineistoja koskevia sääntöjä sovelletaan viranomaisten lisäksi myös elinkeinonharjoittajiin ja heidän palveluksessaan oleviin silloin, kun nämä osallistuvat turvallisuusluokiteltuun hankkeeseen. Valtionhallinnon toimivaltaiset turvallisuusviranomaiset vastaavat siitä, että suomalainen elinkeinoelämä kykenee käsittelemään kansainvälistä turvallisuusluokiteltua tietoa silloin, kun sen haltuun siirtyy vieraan valtion tai kansainvälisen järjestön turvallisuusluokiteltua tietoa. Yleiset kansainväliset vaatimukset on pyritty huomioimaan Suomen kansallisessa turvallisuusauditointikriteeristössä (KATAKRI sekä tätä tukevat erikseen julkaistut liitteet), jota käytetään työkaluna suomalaisten viranomaisten tarkastaessa kotimaisten yritysten ja muiden yhteisöjen turvallisuustason.

3 EUROOPAN UNIONIN TIETOAINEISTO JA SEN KÄSITTELY

Neuvoston turvallisuussäännöt (2013/488/EU) ovat jäsenvaltioiden kannalta keskeisin EU:n turvallisuusluokiteltujen tietojen suojaamista koskeva säädös. Myös muilla EU:n toimielimillä on omia turvallisuussääntöjä, joissa ne ovat sitoutuneet noudattamaan vastaavia turvallisuusvaatimuksia. Neuvoston turvallisuussäännöistä annettu päätös on soveltamisalaltaan laaja. Päätöksessä säädetään muun muassa EU:n asiakirjojen turvallisuusluokittelusta, tietojen käsittelystä, fyysisestä turvallisuudesta, henkilöstöturvallisuudesta, tietojen turvaamisesta tietojärjestelmissä sekä tietojen luovuttamisesta kolmansille valtioille ja kansainvälisille järjestöille.

Komissio antoi 22.3.2022 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi tietoturvallisuudesta unionin toimielimissä, elimissä ja laitoksissa (COM(2022) 119 final). Ehdotuksen tavoitteena on parantaa EU:n turvallisuusluokiteltujen tietojen sekä turvallisuusluokittelemattomien tietojen suojaamista luomalla tietoturvallisuutta koskevat vähimmäissäännöt, joita sovellettaisiin kaikkiin unionin toimielimiin, elimiin ja laitoksiin. Myös neuvoston turvallisuussäännöt ovat parhaillaan uudistettavina.

3.1 Yleisiä periaatteita

EU:n toimielinten asiakirjojen julkisuutta koskevaan säädökseen, ns. avoimuusasetukseen (Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001) sisältyy yleisiä säännöksiä arkaluonteisten EU-asiakirjojen käsittelystä. Avoimuusasetus sisältää perusteet turvallisuusluokitukselle. Tarkemmista EU:n turvallisuusluokitellun tiedon suojaamiseksi toteutettavista menettelyistä ja järjestelyistä säädetään Euroopan unionin toimielinten turvallisuussäännöissä.

EU:n turvallisuusluokiteltuja tietoja on suojattava koko niiden elinkaaren ajan siten, että pystytään estämään ja havaitsemaan niiden vaarantuminen tai katoaminen. Tällaiset turvatoimet liittyvät erityisesti EU:n turvallisuusluokiteltujen tietojen tuottamiseen, rekisteröimiseen, kopioimiseen, kuljettamiseen, säilyttämiseen ja hävittämiseen. EU:n turvallisuusluokitelluille tiedoille annetaan suojaa niiden turvallisuusluokituksen mukaisesti. Mitä korkeampaan turvallisuusluokkaan aineisto kuuluu, sitä tiukempia turvatoimia edellytetään. Suurin osa turvallisuusluokitelluista tiedoista kuuluu alimpaan RESTREINT UE/EU RESTRICTED turvallisuusluokkaan. Turvallisuusluokkiin CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ja erityisesti TRÈS SECRET UE / EU TOP SECRET kuuluvia aineistoja laaditaan harvemmin ja näitä koskevat turvatoimet ovat huomattavasti kireämmät.

3.2 EU:n julkinen tieto

Euroopan unionin tieto on julkista, jos siihen ei kohdistu avoimuusasetuksessa säädettyjä tiedonsaantirajoituksia. Komission ja neuvoston julkiset asiakirjat ilmenevät muun muassa näiden ylläpitämistä julkisista asiakirjarekistereistä.

3.3 LIMITE-asiakirjat

”LIMITE”-merkintä ei ole turvallisuusluokitusta osoittava merkintä, vaan jakelumerkintä. Merkinnällä osoitetaan, että asiakirja on tarkoitettu sisäiseen jakeluun neuvostolle, sen jäsenille, komissiolle ja tietyille muille EU:n toimielimille ja elimille.

Kunkin asiakirjan kohdalla tulee erikseen arvioida, onko asiakirjassa esitetty tieto julkisuuslain mukaan salassa pidettävää vai julkista. Asiakirjan mahdollinen salassapito voi perustua esimerkiksi julkisuuslain 24 §:n 1 momentin 2 kohtaan (kansainväliset suhteet).

LIMITE

Kyseessä on EU:n sisäinen asiakirjan jakelurajoite.

- **toimitiloille** ei aseteta vaatimuksia
- **tietojärjestelmille** ei aseteta vaatimuksia
- **tiedonsiirrolle** ei aseteta vaatimuksia
- tietoa saa siirtää **Internetin** välityksellä ilman salausta
- saa **kopioida** tavallisella kopiokoneella
- saa **lähettää** postitse
- saa **hävittää** paperisilppurilla tai hävityspalvelua käyttäen.

3.4 EU:n turvallisuusluokiteltu tieto

EU:n turvallisuusluokiteltu tieto, josta käytetään kansainvälistä lyhennettä EUCI (*European Union Classified Information*), tarkoittaa mitä tahansa tietoa tai materiaalia, jolle on määritetty jokin EU:n turvallisuusluokka ja jonka aiheeton paljastuminen saattaisi aiheuttaa eritasoista vahinkoa EU:n tai jonkin sen jäsenmaan eduille.

EU:n tiedon turvallisuusluokittelusta vastaa EU:ssa se taho, jonka tiedosta on kyse. **EU:n turvallisuusluokitellun tiedon luokituksen muuttaminen tai poistaminen voi tapahtua vain sen luvalla, jolta tieto on peräisin.**

EU:n turvallisuusluokittelut rinnastetaan Suomen kansalliseen turvallisuusluokitteluun alla olevan taulukon mukaisesti. EU:n ja Suomen kansallisen turvallisuusluokitellun tietoaineiston käsittelyvaatimukset eivät ole kuitenkaan kaikilta osin yhdenmukaiset, sillä EU:n turvallisuusluokitellun tietoaineiston käsittelyä koskevat neuvoston tai EU:n muiden toimielinten, elinten tai laitosten turvallisuussääntöjen vaatimukset.

Euroopan unionin turvallisuusluokka	**EU-lyhenne**	**Suomen vastaava turvallisuusluokka (1101/2019)**
TRÈS SECRET UE / EU TOP SECRET	TS-UE/ EU-TS	ERITTÄIN SALAINEN (TL I) / YTTERST HEMLIG
SECRET UE / EU SECRET	S-UE/EU-S	SALAINEN (TL II) / HEMLIG
CONFIDENTIEL UE / EU CONFIDENTIAL	C-UE/EU-C	LUOTTAMUKSELLINEN (TL III) / KONFIDENTIELL
RESTREINT UE / EU RESTRICTED	R-UE/EU-R	KÄYTTÖ RAJOITETTU (TL IV) / BEGRÄNSAD TILLGÅNG

EU:n asiakirjat on luokiteltava aina vähintään siihen turvallisuusluokkaan, joka vastaa asiakirjan korkeimpaan turvallisuusluokkaan määritellyn osan turvallisuusluokkaa. Asiakirjan eri osat voivat kuulua keskenään eri turvallisuusluokkiin, jolloin ne merkitään mahdollisuuksien mukaan siten, että eri turvallisuusluokkiin kuuluvat osat voidaan tunnistaa. Suurissa tietoaineistoissa on harkittava erikseen, nouseeko asiakokonaisuus luokitukseltaan yksittäistä tietoa korkeampaan turvallisuusluokkaan (ns. kasautumisvaikutus).

HENKILÖSTÖ

EU:n turvallisuusluokiteltua tietoa saa luovuttaa vain sellaisille henkilöille, joilla on viranomaisen hyväksymä työtehtäviin liittyvä tarve kyseiseen tietoon. Henkilön tulee perehtyä EU:n turvallisuusluokitellun tiedon suojaamista koskeviin velvoitteisiin ennen kuin hänelle voidaan luovuttaa kyseistä tietoa.

Mikäli henkilö käsittelee CONFIDENTIAL UE / EU CONFIDENTIAL tai sitä korkeamman tason EU:n turvallisuusluokiteltua tietoa, hänellä tulee tulla kansallisen turvallisuusviranomaisen myöntämä kansainvälinen henkilöturvallisuusselvitys (Personnel Security Clearance, PSC). Työnantajan on määriteltävä PSC-todistusta edellyttävät tehtävät ja pidettävä niistä ajan tasalla olevaa luetteloa. PSC-todistus perustuu suojelupoliisin tai Pääesikunnan turvallisuusselvityslain (726/2014) nojalla tekemään turvallisuusselvitykseen. PSC-todistusta ja turvallisuusselvitystä ei edellytetä niistä henkilöistä, joille luovutetaan tarpeeseen perustuen korkeintaan RESTREINT UE / EU RESTRICTED -luokan tietoa. PSC-todistus on tehtäväkohtainen ja tulee aina uusia tehtävän vaihtuessa, vaikka turvallisuusselvitys olisi pidempään voimassa. Ks. tarkemmin:

Linkki NSA:n sivulle, josta löytyy ohje PSC-todistuksen hakemisesta

Kaikille henkilöille, jotka siirtyvät pois tehtävistä, jotka ovat edellyttäneet pääsyä EU:n turvallisuusluokiteltuihin tietoihin, on selvitettävä heidän velvollisuutensa luokiteltujen tietojen jatkuvan suojaamisen osalta, ja heidän on tarvittaessa annettava siitä kirjallinen vakuutus.

TILAT

Fyysinen turvallisuus on mitoitettava siten, että EU:n turvallisuusluokiteltuun tietoon ei ole mahdollisuutta päästä käsiksi oikeudetta. Vaatimus koskee kaikkia tiloja, joissa EU:n turvallisuusluokiteltua tietoa käsitellään tai säilytetään. Toimivaltaisen viranomaisen hyväksyntää edellytetään tilojen osalta riippuen turvallisuusluokan tasosta. EU:n turvallisuusluokitellun tiedon käsittely on turvallisuusluokasta riippuen mahdollista kolmella eritasoisella alueella:

- pääsynhallinnan piiriin kuuluvat **hallinnolliset alueet**,
- tiukemman pääsynhallinnan piiriin kuuluvat varsinaiset **turva-alueet** ja
- **teknisin keinoin suojatut turva-alueet**, joissa salakuuntelu on estetty.

JÄRJESTELMÄT

Tietojärjestelmien, joissa EU:n turvallisuusluokiteltua tietoa käsitellään, tulee läpikäydä hyväksyntäprosessi (akkreditointi). Hyväksyntäprosessin päätteeksi toimivaltainen hyväksyntäviranomainen (SAA, Security Accreditation Authority, Suomessa NCSA-FI) laatii tietojärjestelmälle hyväksyntälausunnon. Tietojärjestelmissä, joissa käsitellään vähintään turvallisuusluokan CONFIDENTIEL UE / EU CONFIDENTIAL -tietoa, tulee lisäksi huomioida sähkömagneettisen hajasäteilyn vaarat ja toteuttaa keinot niiden minimoimiseksi (ns. TEMPEST-toimet).

Kun EU:n turvallisuusluokiteltua tietoa siirretään fyysisten turvallisuusalueiden ulkopuolella tai matalamman turvallisuusluokan tietoverkon kautta, tulee tieto suojata hyväksytyllä salaustuotteella. Suojaamiseen tulee käyttää EU:n neuvoston hyväksymää salaustuotetta. Luokkien RESTREINT UE / EU RESTRICTED ja CONFIDENTIEL UE / EU CONFIDENTIAL tietojen suojaamiseen voidaan käyttää myös kansallisen salaustuotteiden hyväksyntäviranomaisen (CAA, Crypto Approval Authority, Suomessa NCSA-FI) hyväksymiä salaustuotteita.

3.4.1 RESTREINT UE / EU RESTRICTED

Kyseessä on turvallisuusluokka, jonka mukaan

- **henkilöllä** tulee olla viranomaisen hyväksymä, työtehtävään liittyvä tarve turvallisuusluokiteltuun tietoon (need-to-know)
- henkilön tulee **perehtyä** turvallisuusluokan mukaisiin velvoitteisiin
- henkilölle tulee säännöllisin väliajoin tiedottaa EU:n turvallisuusluokiteltuun tietoon ja tiedon käsittelyyn liittyvistä turvallisuusuhkista

- RESTREINT UE / EU RESTRICTED -luokan aineistoa voidaan **käsitellä** turva-alueella tai hallinnollisella alueella, jos pääsy tietoihin on suojattu sivullisilta.
- RESTREINT UE / EU RESTRICTED luokan aineistoa tulee **säilyttää** lukitussa paikassa hallinnollisella alueella tai turva-alueella, eivätkä sivulliset saa päästä tutustumaan aineistoon

- **tietojärjestelmä** tulee erikseen hyväksyttää toimivaltaisella viranomaisella (SAA, Suomessa NCSA-FI)
- kansallisten tietoverkkojen liittäminen EU:n luokiteltuun tietoverkkoon tulee hyväksyttää kansallisella toimivaltaisella viranomaisella (SAA, NCSA-FI)
- **tietoa sähköisesti siirrettäessä** salausmenetelmän tulee olla EU:n turvallisuusviranomaisen tai kansallisen toimivaltaisen viranomaisen (CAA, Suomessa NCSA-FI) hyväksymä
- tietoa **ei saa siirtää Internetin** välityksellä, ellei tieto ole salattu toimivaltaisen viranomaisen tarkoitukseen erikseen hyväksymällä salaamismenetelmällä
- saa **kopioida** vain toimivaltaisen viranomaisen (NCSA-FI) ko. turvallisuusluokan tietojen kopiointiin hyväksymällä (akkreditoidulla) kopiokoneella

- saa **lähettää** postitse läpinäkymättömässä kirjekuoressa
- saa **kuljettaa** rakennuksen tai suljetun rakennusryhmän sisällä edellyttäen, että tiedot on peitetty niin, ettei niiden sisältö ole havaittavissa
- saa **kuljettaa** unionin alueella sekä kolmannen valtion alueelle edellyttäen, että tiedot on pakattu niin, että tieto on suojattu luvattomalta ilmitulolta
- saa **hävittää** paperisilppurilla tai hävityspalvelua käyttäen, mikäli paperisilppuri täyttää ko. turvallisuusluokan vaatimukset tai hävityspalvelu on viranomaisten hyväksymä.

3.4.2 CONFIDENTIEL UE / EU CONFIDENTIAL

Kyseessä on turvallisuusluokka, jonka mukaan

- **henkilöllä** tulee olla viranomaisen hyväksymä, työtehtävään liittyvä **tarve** turvallisuusluokiteltuun tietoon (need-to-know)
- henkilöllä tulee olla riittävän tasoinen kansainvälinen **henkilöturvallisuustodistus (PSCC)**
- henkilön tulee **perehtyä** turvallisuusluokan mukaisiin velvoitteisiin ja hänen tulee kirjallisesti vakuuttaa tiedostavansa tietojen suojaamista koskevat vastuunsa
- henkilölle tulee säännöllisin väliajoin tiedottaa EU:n turvallisuusluokiteltuun tietoon ja tiedon käsittelyyn liittyvistä turvallisuusuhkista
- työnantajan on myönnettävä henkilölle kirjallisesti **oikeus** CONFIDENTIEL UE / EU CONFIDENTIAL -luokan tiedon käsittelyyn

- CONFIDENTIEL UE / EU CONFIDENTIAL -luokan tietoa voidaan **käsitellä** turva-alueella tai hallinnollisella alueella, mikäli pääsy tietoihin on suojattu sivullisilta. Huolehdittava, ettei tilaan ole näköyhteyttä ulkopuolelta
- CONFIDENTIEL UE / EU CONFIDENTIAL -luokan tieto tulee **säilyttää** turva-alueella kansallisesti hyväksytyssä kassakaapissa aina huonetilasta poistuttaessa, ellei tila ole tarkoitukseen hyväksytty, hälytysjärjestelmällä varustettu holvi

- **tietojärjestelmä** tulee erikseen hyväksyttää toimivaltaisella viranomaisella (SAA, Suomessa NCSA-FI)
- kansallisten tietoverkkojen liittäminen EU:n luokiteltuun tietoverkkoon tulee hyväksyttää kansallisella toimivaltaisella viranomaisella (SAA, NCSA-FI)
- mikäli CONFIDENTIEL UE / EU CONFIDENTIAL -luokan tietoa käsitellään sähköisesti, sähkömagneettinen hajasäteily on estettävä riittävän tehokkaasti (ns. TEMPEST-toimet)
- tietoa **sähköisesti siirrettäessä** salausmenetelmän tulee olla EU:n turvallisuusviranomaisen tai kansallisen toimivaltaisen viranomaisen (CAA, NCSA-FI) hyväksymä
- tietoa ei saa siirtää **Internetin** välityksellä, ellei tieto ole salattu toimivaltaisen viranomaisen tarkoitukseen erikseen hyväksymällä salaamismenetelmällä
- saa **kopioida** vain toimivaltaisen viranomaisen (NCSA-FI) ko. turvallisuusluokan tietojen kopiointiin hyväksymällä (akkreditoidulla) kopiokoneella

- **rekisteröitävä** ennen lähettämistä, vastaanotettaessa ja hävitettäessä

- saa **lähettää** EU:n alueella kaupallista kuriiripalvelua koskevien vaatimusten mukaisesti kirjattuna kahdessa läpinäkymättömässä kirjekuoressa tai lukitussa ja/tai sinetöidyssä kuljetuspussissa. Uloimmassa kuoressa ei saa olla merkintää turvallisuusluokituksesta. Unionin alueelta kolmanteen valtioon ainoastaan kuriiritse

- **kuljetetaan** pääsääntöisesti sotilaskuriirilla, valtion kuriirilla tai diplomaattikuriirilla
- saa kuljettaa unionin alueella sekä kolmannen valtion alueelle edellyttäen, että tiedot on pakattu niin, että tieto on suojattu luvattomalta ilmitulolta, tiedot ovat koko ajan kuljettajansa hallussa eikä tietoja avata matkalla, tietoa kuljettavalla henkilöllä on asianmukaisen tason PSC-todistus sekä kansallisen turvallisuusviranomaisen myöntämä kuriiritodistus ja aineiston kuljetuksessa noudatetaan kansallisen turvallisuusviranomaisen tilannekohtaista lisäohjeistusta

- CONFIDENTIEL UE / EU CONFIDENTIAL –luokan tietoaineisto **hävitetään aineistosta vastaavassa rekisterissä** asiakirjan haltijan tai toimivaltaisen viranomaisen määräyksestä. Vastuurekisterin asiaa koskevat kirjaustiedot on päivitettävä samassa yhteydessä
- CONFIDENTIEL UE / EU CONFIDENTIAL –luokan tietoaineiston hävittämisestä tulee laatia **hävittämistodistus**, jota säilytetään vastuurekisterissä vähintään viiden vuoden ajan.

3.4.3 SECRET UE / EU SECRET

Kyseessä on turvallisuusluokka, jonka mukaan

- **henkilöllä** tulee olla viranomaisen hyväksymä, **työtehtävään liittyvä tarve** turvallisuusluokiteltuun tietoon (need-to-know)
- henkilöllä tulee olla riittävän tasoinen kansainvälinen **henkilöturvallisuustodistus (PSCC)**
- henkilön tulee **perehtyä** turvallisuusluokan mukaisiin velvoitteisiin ja hänen tulee kirjallisesti vakuuttaa tiedostavansa tietojen suojaamista koskevat vastuunsa
- henkilölle tulee säännöllisin väliajoin tiedottaa EU:n turvallisuusluokiteltuun tietoon ja tiedon käsittelyyn liittyvistä turvallisuusuhkista
- työnantajan on myönnettävä henkilölle kirjallisesti **oikeus** SECRET UE / EU SECRET -luokan tiedon käsittelyyn

- SECRET UE / EU SECRET -luokan tietoa voidaan **käsitellä** turva-alueella tai hallinnollisella alueella, mikäli pääsy tietoihin on suojattu sivullisilta. Huolehdittava, ettei tilaan ole näköyhteyttä ulkopuolelta
- SECRET UE / EU SECRET -luokan tieto tulee **säilyttää** turva-alueella kansallisesti hyväksytyssä kassakaapissa aina huonetilasta poistuttaessa, ellei tila ole tarkoitukseen hyväksytty, hälytysjärjestelmällä varustettu holvi

- **tietojärjestelmä** tulee hyväksyttää erikseen toimivaltaisella viranomaisella (NCSA-FI)
- kansallisten tietoverkkojen liitännät EU:n luokiteltuun tietoverkkoon tulee hyväksyttää kansallisella toimivaltaisella viranomaisella (SAA, NCSA-FI)
- mikäli SECRET UE / EU SECRET -luokan tietoa käsitellään sähköisesti, sähkömagneettinen hajasäteily on estettävä riittävän tehokkaasti (ns. TEMPEST-toimet)
- tietoa **sähköisesti siirrettäessä** salausmenetelmän tulee olla EU:n neuvoston hyväksyntäviranomaisen hyväksymä. Tietoa ei saa siirtää **Internetin** välityksellä, ellei tieto ole salattu tarkoitukseen EU:n turvallisuusviranomaisten nimenomaisesti hyväksymällä salaamismenetelmällä
- saa **kopioida** vain toimivaltaisen viranomaisen (NCSA-FI) ko. turvallisuusluokan tietojen kopiointiin hyväksymällä (akkreditoidulla) kopiokoneella

- **rekisteröitävä** ennen lähettämistä, vastaanotettaessa ja hävitettäessä

- **kuljetetaan** pääsääntöisesti sotilaskuriirilla, valtion kuriirilla tai diplomaattikuriirilla
- saa kuljettaa unionin alueella sekä kolmannen valtion alueelle edellyttäen, että tiedot on pakattu niin, että tieto on suojattu luvattomalta ilmitulolta, tiedot ovat koko ajan kuljettajansa hallussa eikä tietoja avata matkalla, tietoa kuljettavalla henkilöllä on asianmukaisen tason PSC-todistus sekä kansallisen turvallisuusviranomaisen myöntämä kuriiritodistus ja aineiston kuljetuksessa noudatetaan kansallisen turvallisuusviranomaisen tilannekohtaista lisäohjeistusta

- SECRET UE / EU SECRET -luokan tietoaineisto **hävitetään** aineistosta vastaavassa rekisterissä asiakirjan haltijan tai toimivaltaisen viranomaisen määräyksestä. Vastuurekisterin asiaa koskevat kirjaustiedot on päivitettävä samassa yhteydessä
- hävittäminen suoritettava **todistajan läsnä ollessa** ja todistajalla oltava vähintään hävitettävän asiakirjan turvallisuusluokkaa vastaava PSC-todistus.
- SECRET UE / EU SECRET -luokan tietoaineiston hävittämisestä tulee laatia **hävittämistodistus**, jota säilytetään vastuurekisterissä vähintään viiden vuoden ajan

3.4.4 TRÈS SECRET UE / EU TOP SECRET

TRÈS SECRET UE / EU TOP SECRET -asiakirjojen laatiminen ja käsittely EU:ssa ja sen jäsenmaissa on hyvin harvinaista. Niiden käsittelyssä edellytetään SECRET UE / EU SECRET -luokan vaatimuksia, mutta käsittelijän henkilövalintaan liittyy lisäksi erikseen ratkaistavia erityistoimenpiteitä (käsittelyoikeudet ja turvallisuusselvitystasomäärittelyt). Lisäksi kyseisen luokan asiakirjojen rekisteröinti, kuljetus ja hävittäminen poikkeavat alemmista turvallisuusluokista (edellyttää aina TRÈS SECRET UE / EU TOP SECRET – keskuskirjaamon myötävaikutusta), eikä tämän turvallisuusluokan tietojärjestelmästä saa olla suoria tai porrastettuja yhteyksiä suojaamattomiin verkkoihin.

4 NATON TIETOAINEISTO JA SEN KÄSITTELY

Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta tehty sopimus (SopS 55 ja 56/2023) on tullut Suomen osalta voimaan 23.8.2023. Sopimus korvaa Suomen ja Naton välisen aiemman tietoturvallisuussopimuksen ja sitä täydentäneen järjestelyn (SopS 7 ja 8/2013). Sopimuksen mukaan osapuolet suojaavat ja turvaavat Naton luovuttamaa turvallisuusluokiteltua tietoa ja jäsenmaiden Natolle toimittamaa turvallisuusluokiteltua tietoa. Osapuolten suojelevat myös jäsenvaltioiden välillä Naton ohjelman, hankkeen tai sopimuksen tueksi vaihdettua turvallisuusluokiteltua tietoa.

Suomen viranomaisten asiakirjoihin sovelletaan julkisuusperiaatetta. Naton asiakirjoihin julkisuusperiaatetta ei järjestön omien säännösten tai käytäntöjen perusteella sovelleta. Voimassa oleva Naton turvallisuussäännöstö pohjautuu dokumentaatiokokonaisuuteen, josta käytetään nimitystä *Nato Security Policy* (NSP). Yhteisen suojauksen tason periaatteet ja vähimmäisvaatimukset sisältyvät Naton asiakirjaan C-M(2002)49-REV1. Turvallisuussäännöstön käytännön ylläpitotyön toteuttaa Naton turvallisuustoimisto NOS (*Nato Office of Security*).

Mikäli Natolle luovutettu tieto on turvallisuusluokiteltua, tiedon luovuttaneen maan määräysvalta asiakirjaan säilyy, eikä tietoa voida Natossa luokitella uudestaan ilman sen luovuttaneen maan kirjallista lupaa.

Nato edellyttää jäsenmailtaan ja sopimuskumppanimailtaan keskitettyä turvallisuusluokitellun tiedon hallintaa. Tämä tarkoittaa rekisterijärjestelmän perustamista. Rekisterijärjestelmään kuuluu yleensä keskusrekisteri(t), alarekistereitä ja mahdollisia erillisrekistereitä ja kontrollipisteitä

4.1 Naton julkinen tieto

Julkista on sellainen Naton tieto, jota ei ole turvallisuusluokiteltu ja jonka asiasta vastuussa oleva Naton toimielin tai virasto julkaisee.

4.2 Naton luokittelematon tieto

Naton sisäiseen käyttöön tarkoitettu tieto, jota ei ole turvallisuusluokiteltu, merkitään merkinnällä NATO UNCLASSIFIED (NU). Tällaiseen tietoon voi liittyä myös hallinnollinen merkintä (esim. NATO UNCLASSIFIED MEDICAL) tai jakelurajoitemerkintä (esim. NATO UNCLASSIFIED Releasable to OSCE (tai muu vastaanottaja) ONLY. Tällaista tietoa saa luovuttaa

Naton turvallisuussäännöstön mukaan vain henkilöille, joilla on työtehtävään liittyvä, viranomaisen hyväksymä tarve tietoon. Asiakirjan ollessa Suomen viranomaisen hallussa, arvioidaan kunkin asiakirjan julkisuutta tapauskohtaisesti julkisuuslain perusteella. NATO UNCLASSIFIED merkinnällä varustetun asiakirjan mahdollinen salassapito voi perustua esimerkiksi julkisuuslain 24 §:n 1 momentin 2 kohtaan. Tiedon alkuperäisen luovuttajan tekemiä hallinnollisia tai jakelurajoitus merkintöjä voi kuitenkin muuttaa ainoastaan tiedon alkuperäinen luovuttaja.

NATO UNCLASSIFIED

- **henkilöllä** tulee olla viranomaisen hyväksymä, työtehtävään liittyvä tarve tietoon ja hänen tulee ymmärtää asiakirjan käsittelyä koskevien rajoitteiden merkitys
- **toimitiloille** ei aseteta vaatimuksia
- **tietojärjestelmille** ei aseteta erityisiä vaatimuksia, mutta niiden tulee turvata tiedon eheys, saatavuus ja luottamuksellisuus sekä tarjota keinot tunnistaa ja varmentaa käyttäjät, joilla on pääsyoikeus tällaiseen tietoon
- **tiedonsiirrolle** ei aseteta vaatimuksia
- voidaan siirtää **Internetin** välityksellä salaamattomana
- saa **kopioida** tavallisella kopiokoneella
- saa **lähettää** postitse
- saa **hävittää** paperisilppurilla tai hävityspalvelua käyttäen
- saa luovuttaa Naton ulkopuoliselle taholle ainoastaan, mikäli tämä taho käy nimenomaisesti ilmi alkuperäisen luovuttajan jakelurajoitusmerkinnästä tai mikäli tiedon alkuperäisen luovuttaja antaa erikseen tähän luvan.

4.3 Naton turvallisuusluokiteltu tieto

Naton turvallisuusluokiteltu tieto tarkoittaa mitä tahansa tietoa tai materiaalia, jolle on määritetty jokin Naton turvallisuusluokka ja jonka aiheeton paljastuminen saattaisi aiheuttaa eritasoista vahinkoa Naton tai jonkin sen jäsenmaan eduille.

MERKINNÄT

Naton turvallisuusluokittelut rinnastetaan Suomen kansalliseen turvallisuusluokitteluun alla olevan taulukon mukaisesti. Naton ja Suomen kansallisen turvallisuusluokitellun tietoaineiston käsittelyvaatimukset eivät olen kuitenkaan kaikilta osin yhdenmukaiset, sillä Naton turvallisuusluokitellun tietoaineiston käsittelyä koskevat Naton turvallisuussäännöstön vaatimukset.

Naton turvallisuusluokka	Lyhenne	Suomen vastaava turvallisuusluokka (1101/2019)
COSMIC TOP SECRET	CTS	ERITTÄIN SALAINEN (TL I) / YTTERST HEMLIG
NATO SECRET	NS	SALAINEN (TL II) / HEMLIG
NATO CONFIDENTIAL	NC	LUOTTAMUKSELLINEN (TL III) / KONFIDENTIELL
NATO RESTRICTED	NR	KÄYTTÖ RAJOITETTU (TL IV)/ BEGRÄNSAD TILLGÅNG

Turvallisuusluokkamerkintä liitetään Naton asiakirjoihin jokaiselle sivulle sekä sivun yläettä alalaitaan. Merkintä tehdään lisäksi viimeisen sivun kääntöpuolelle. Naton asiakirjat on luokiteltava aina vähintään siihen turvallisuusluokkaan, joka vastaa asiakirjan korkeinta luokittelua sisältävää tietoa. Suurissa tietoaineistoissa on harkittava erikseen, nouseeko asiakokonaisuus luokitukseltaan yksittäistä tietoa korkeampaan turvallisuusluokkaan (ns. kasautumisvaikutus).

Nato-tiedon asianmukaisesta turvallisuusluokittelusta vastaa asiakirjan laatinut taho. Turvallisuusluokitellun Nato-tiedon luokituksen laskeminen tai julistaminen julkiseksi tiedoksi voi tapahtua vain asiakirjan laatineen etukäteen antamalla kirjallisella luvalla.

JAKELUMERKINNÄT

Naton turvallisuusluokitellun tiedon jakelua voidaan hallita ja rajoittaa turvallisuusluokkamerkinnän yhteyteen sijoitettavien jakelumerkintöjen avulla. Tämä tulee kysymykseen erityisesti silloin, kun asiakirja tai materiaali jaetaan ns. kolmannelle osapuolelle. Seuraavassa on kolme esimerkkiä turvallisuusluokittelu- ja jakelumerkintöjen käytöstä:

1. Kohdeorganisaatio tai operaatio ja turvallisuusluokitus, esimerkiksi

ISAF CONFIDENTIAL

2. Jos pääsy ko. tietoaineistoon on rajoitettu vain tietyille rauhankumppanuusmaille, on merkintä esim.

NATO / PfP RESTRICTED
AUSTRIA ONLY

3. Jos pääsy ko. tietoaineistoon on sallittu esim. kaikille tiettyyn kriisinhallintaope-raatioon osallistuville valtioille, on merkintä esim.

NATO / CONFIDENTIAL
RELEASABLE to KFOR

ERITYISLUOKAT Luokiteltu tieto voi kuulua myös erityisluokkiin. ATOMAL-merkinnällä varustettua tietoa on suojattava Pohjois-Atlantin sopimuksen osapuolten välillä ydinpuolustustietoja koskevasta yhteistyöstä tehdyn sopimuksen ja sitä tukevien hallinnollisten järjestelyjen mukaisesti (ei vielä Suomen osalta voimassa). CRYPTO-merkinnällä varustetaan COMSEC-avainmateriaaliin liittyvä tieto, jota on suojattava Naton salausturvallisuusperiaatteiden ja –ohjeiden mukaisesti. BOHEMIA-merkinnällä varustetaan viestitiedustelusta saatu tai siihen liittyvä erityisluokan tieto.

HENKILÖSTÖ **Naton turvallisuusluokiteltua tietoa saa luovuttaa vain sellaisille henkilöille, joilla on kansallisen viranomaisen hyväksymä tarve kyseiseen tietoon**. Henkilön tulee perehtyä Naton turvallisuusluokitellun tiedon suojaamista koskeviin velvoitteisiin, ennen kuin hänelle voidaan luovuttaa kyseistä tietoa.

Mikäli henkilö käsittelee NATO CONFIDENTIAL tai sitä korkeamman tason Naton turvallisuusluokiteltua tietoa, hänellä tulee olla kansallisen turvallisuusviranomaisen myöntämä kansainvälinen henkilöturvallisuustodistus (Personnel Security Clearance Certificate, PSCC). Työnantajan on määriteltävä PSC-todistusta edellyttävät tehtävät ja pidettävä tästä ajan tasalla olevaa luetteloa. PSC-todistus perustuu suojelupoliisin tai pääesikunnan turvallisuusselvityslain nojalla tekemään turvallisuusselvitykseen. PSC-todistusta ja turvallisuusselvitystä ei edellytetä niistä henkilöistä, joille luovutetaan viralliseen tarpeeseen perustuen korkeintaan NATO RESTRICTED -luokan tietoa, mutta henkilön tulee kirjallisesti vakuuttaa tiedostavansa tietojen suojaamista koskevat vastuunsa ennen kuin hänelle voidaan luovuttaa kyseistä tietoa. PSC-todistus on tehtäväkohtainen ja tulee aina uusia tehtävän vaihtuessa, vaikka turvallisuusselvitys olisi pidempään voimassa. Ks. tarkemmin:

Linkki NSA:n sivuille, josta löytyy ohje PSC-todistuksen hakemisesta

Kaikille henkilöille, jotka siirtyvät pois tehtävistä, jotka ovat edellyttäneet pääsyä Naton turvallisuusluokiteltuihin tietoihin, on selvitettävä heidän velvollisuutensa turvallisuusluokiteltujen tietojen jatkuvan suojaamisen osalta Naton turvallisuussäännöstön mukaisesti.

TILAT **Fyysinen turvallisuus** on mitoitettava siten, että Naton turvallisuusluokiteltuun tietoon ei ole mahdollisuutta päästä käsiksi oikeudetta. Vaatimus koskee kaikkia niitä tiloja, joissa Naton turvallisuusluokiteltua tietoa käsitellään tai säilytetään. NATO RESTRICTED -tiedon käsittelyn sekä säilytyksen tulee tapahtua hallinnollisella alueella tai turva-alueella. Mikäli

käsiteltävän tiedon luokka on vähintään NATO CONFIDENTIAL, tulee tiedon käsittelyn ja säilytyksen rajoittua turva-alueelle.

JÄRJESTELMÄT **Tietojärjestelmien**, joissa Naton turvallisuusluokiteltua tietoa käsitellään, tulee läpikäydä hyväksyntäprosessi (akkreditointi). Hyväksyntäprosessin päätteeksi toimivaltainen hyväksyntäviranomainen (SAA, Security Accreditation Authority, Suomessa NCSA-FI) laatii tietojärjestelmälle hyväksyntälausunnon. Tietojärjestelmissä, joissa käsitellään vähintään turvallisuusluokan NATO CONFIDENTIAL -tietoa, tulee lisäksi huomioida sähkömagneettisen hajasäteilyn vaarat ja etsiä keinot niiden minimoimiseksi (ns. TEMPEST-toimet).

Kun Naton turvallisuusluokiteltua tietoa siirretään fyysisten turvallisuusalueiden ulkopuolella tai matalamman turvallisuusluokan tietoverkon kautta, tulee tieto suojata hyväksytyllä salaustuotteella. Luokkien NATO SECRET ja COSMIC TOP SECRET tietojen suojaamiseen tulee käyttää Naton sotilaskomitean hyväksymiä salaustuotteita. Luokkien NATO RESTRICTED ja NATO CONFIDENTIAL tietojen suojaamiseen voidaan käyttää myös kansallisen toimivaltaisen hyväksyntäviranomaisen (NCSA-FI) hyväksymiä salaustuotteita.

4.3.1 NATO RESTRICTED

Kyseessä on turvallisuusluokka, jonka mukaan

- **henkilöllä** tulee olla viranomaisen hyväksymä, työtehtävään liittyvä tarve turvallisuusluokiteltuun tietoon (need-to-know)
- henkilö tulee ohjeistaa NATO RESTRICTED –luokan aineiston käsittelyyn liittyvistä turvallisuusmenettelyistä ja turvallisuusvelvoitteistaan, ja henkilön tulee vakuuttaa ymmärtävänsä vastuunsa ja häneen mahdollisesti kohdistuvat seuraukset, mikäli Naton turvallisuusluokiteltua tietoa joutuu luvattomiin käsiin
- henkilölle tulee säännöllisin väliajoin tiedottaa turvallisuusluokiteltuun tietoon ja tällaisen tiedon käsittelyyn liittyvistä turvallisuusuhkista

- **toimitilan**, jossa NATO RESTRICTED -luokan tietoa käsitellään ja säilytetään, tulee olla pääsynhallinnan piirissä oleva hallinnollinen alue tai luokan I tai II turva-alue. Aineisto on säilytettävä alueella vähintään lukitussa kaapissa tai toimistokalusteessa, eivätkä sivulliset saa päästä tutustumaan aineistoon

- **tietojärjestelmä** tulee erikseen hyväksyttää toimivaltaisella viranomaisella

- tietoa **sähköisesti siirrettäessä** salausmenetelmän tulee olla Naton tai toimivaltaisen viranomaisen hyväksymä
- tietoa ei saa siirtää **Internetin** välityksellä, ellei tieto ole salattu tarkoitukseen erikseen hyväksytyllä salaamismenetelmällä
- saa **kopioida** vain toimivaltaisen viranomaisen (NCSA-FI) ko. turvallisuusluokan tietojen kopiointiin hyväksymällä (akkreditoidulla) kopiokoneella

- saa **lähettää** postitse läpinäkymättömässä kirjekuoressa tai pakkauksessa, kuoren tai pakkauksen merkinnöistä ei käy ilmi aineiston turvallisuusluokka
- saa **kuljettaa** vähintään yhdessä läpinäkymättömässä kirjekuoressa tai pakkauksessa. Kuoren tai pakkauksen merkinnöistä ei saa käydä ilmi aineiston turvallisuusluokka ja kuljetuksen aikana on huolehdittava suojauksesta
- saa **hävittää** paperisilppurilla tai hävityspalvelua käyttäen, mikäli paperisilppuri täyttää ko. turvallisuusluokan vaatimukset tai hävityspalvelu on viranomaisten hyväksymä.

4.3.2 NATO CONFIDENTIAL

Kyseessä on turvallisuusluokka, jonka mukaan

- **henkilöllä** tulee olla viranomaisen hyväksymä, työtehtävään liittyvä **tarve** turvallisuusluokiteltuun tietoon (need-to-know)
- henkilöllä tulee olla riittävän tasoinen kansainvälinen **henkilöturvallisuustodistus (PSCC)**
- henkilö **tulee ohjeistaa** aineiston käsittelyyn liittyvistä turvallisuusmenettelyistä ja –velvoitteistaan ja henkilön tulee kirjallisesti vakuuttaa ymmärtävänsä vastuunsa ja häneen mahdollisesti kohdistuvat seuraukset, mikäli Naton turvallisuusluokiteltua tietoa joutuu luvattomiin käsiin
- henkilölle tulee säännöllisin väliajoin tiedottaa turvallisuusluokiteltuun tietoon ja tällaisen tiedon käsittelyyn liittyvistä turvallisuusuhkista
- työnantajan on myönnettävä henkilölle kirjallisesti **oikeus** NATO CONFIDENTIAL -luokan tiedon käsittelyyn

- **toimitilan**, jossa NATO CONFIDENTIAL -luokan tietoa käsitellään, tulee olla pääsynhallinnan piirissä oleva fyysisesti suojattu luokan I tai II turva-alue. Tietoa käsiteltäessä pääsy tietoihin on suojattava sivullisilta. Huolehdittava, ettei tilaan ole näköyhteyttä ulkopuolelta
- NATO CONFIDENTIAL -luokan tieto tulee säilyttää luokan I tai luokan II turva-alueella kansallisesti hyväksytyssä kassakaapissa aina turva-alueelta poistuttaessa

- **tietojärjestelmä** tulee erikseen hyväksyttää toimivaltaisella viranomaisella
- mikäli NATO CONFIDENTIAL -luokan tietoa käsitellään sähköisesti, sähkömagneettinen hajasäteily on estettävä riittävän tehokkaasti (ns. TEMPEST-toimet)
- tietoa **sähköisesti siirrettäessä** salaustuotteen tulee olla Naton sotilaskomitean tai kansallisen toimivaltaisen viranomaisen (NCSA-FI) hyväksymä
- tietoa ei saa siirtää **Internetin** välityksellä, ellei tieto ole salattu tarkoitukseen erikseen hyväksytyllä salaamismenetelmällä
- saa **kopioida** vain toimivaltaisen viranomaisen (NCSA-FI) ko. turvallisuusluokan tietojen kopiointiin hyväksymällä (akkreditoidulla) kopiokoneella
- Naton säännöt eivät edellytä jäsenmailta NATO CONFIDENTIAL –tietoaineiston rekisteröintiä ennen lähettämistä ja vastaanotettaessa, mutta Suomessa myös tämä aineisto tulee rekisteröidä kansallisen sääntelyn

nojalla (ks. turvallisuusluokitteluasetuksen 14 § ja tiedonhallintalain 25 §)

- NATO CONFIDENTIAL –tietoaineisto **kuljetetaan** pääsääntöisesti sotilaskuriirilla, valtion kuriirilla tai diplomaattipostina
- tietoaineiston fyysistä kuljettamista tulisi välttää, jos tieto voidaan siirtää turvallisesti sähköisesti
- saa **kuljettaa** Nato-jäsenvaltion sisällä rakennelmien välillä henkilökohtaisesti kuriirivelvoittein edellyttäen, että:
    - aineisto on pakattu vähintään kahteen läpinäkymättömään kuoreen
    - pakkaus estää tiedon luvattoman ilmitulon
    - tietoaineiston turvallisuusluokka ja vastaanottaja käyvät ilmi vain pakkauksen sisimmästä kuoresta
    - ulompi kuori sisältää vastaanottajan tiedot (ei aineiston turvallisuusluokkaa) sekä mekanismin, jolla toimituksen toteutus voidaan dokumentoida
    - kuljetusvälinettä (salkku tms.) ei saa jättää missään oloissa vartioimatta ja sen tulee olla lukittu
    - lähetys tulee avata dokumentoidusti määränpäässä, tietoa ei saa avata kuljetuksen aikana
    - henkilökuriirilla tulee olla asianmukaisen tason PSC-todistus, hänen tulee perehtyä Naton turvallisuusmääräyksiin ja hänellä tulee olla kansallisten määräysten mukainen valtuutus sekä Naton säännösten mukainen henkilökuriiritodistus.

- saa **kuljettaa** Nato-valtioiden sekä kolmansien valtioiden välillä henkilökohtaisesti, mutta tämä edellyttää edellä lueteltujen vaatimusten noudattamisen lisäksi aina kansallisen turvallisuusviranomaisen erityisohjeistusta sekä myötävaikutusta

- saa **hävittää** kyseisen turvallisuusluokan vaatimukset täyttävällä paperisilppurilla

4.3.3 NATO SECRET

Kyseessä on turvallisuusluokka, jonka mukaan

- **henkilöllä** tulee olla viranomaisen hyväksymä, työtehtävään liittyvä **tarve** turvallisuusluokiteltuun tietoon (need-to-know)
- henkilöllä tulee olla riittävän tasoinen kansainvälinen **henkilöturvallisuustodistus (PSCC)**
- henkilö **tulee ohjeistaa** aineiston käsittelyyn liittyvistä turvallisuusmenettelyistä ja –velvoitteistaan ja henkilön tulee kirjallisesti vakuuttaa ymmärtävänsä vastuunsa ja häneen mahdollisesti kohdistuvat seuraukset, mikäli Naton turvallisuusluokiteltua tietoa joutuu luvattomiin käsiin
- henkilölle tulee säännöllisin väliajoin tiedottaa turvallisuusluokiteltuun tietoon ja sen käsittelyyn liittyvistä turvallisuusuhkista
- työnantajan on myönnettävä henkilölle kirjallisesti **oikeus** NATO SECRET -luokan tiedon käsittelyyn

- **toimitilaan** pääsyä tulee valvoa siten, että järjestelyllä estetään muita kuin NATO SECRET -luokan aineiston käsittelyoikeuden omaavia pääsemästä tilaan valvomatta. Tilan tulee olla NATO SECRET -luokan tiedon käsittelyyn hyväksytty luokan I tai luokan II turva-alue
- NATO SECRET -luokan tieto tulee säilyttää kansallisesti hyväksytyssä kassakaapissa aina turva-alueelta poistuttaessa, ellei tila ole tarkoitukseen hyväksytty, hälytysjärjestelmällä varustettu holvi
- huolehdittava, ettei tilaan ole näköyhteyttä ulkopuolelta silloin, kun käsitellään NATO SECRET -luokan aineistoa

- **tietojärjestelmät,** joilla Naton turvallisuusluokiteltua tietoa siirretään tai käsitellään, tulee erikseen hyväksyttää (akkreditoida) toimivaltaisella turvallisuusviranomaisella (SAA, NCSA-FI).
- mikäli NATO SECRET -luokan tietoa käsitellään sähköisesti, sähkömagneettinen hajasäteily on estettävä riittävän tehokkaasti (ns. TEMPEST-toimet)
- tietoa **sähköisesti siirrettäessä** salausmenetelmän tulee olla Naton sotilaskomitean erikseen hyväksymä
- tietoa ei saa siirtää **Internetin** välityksellä, ellei tieto ole salattu Naton sotilaskomitean tähän nimenomaiseen tarkoitukseen erikseen hyväksymällä salaamismenetelmällä
- saa **kopioida** vain toimivaltaisen viranomaisen (NCSA-FI) ko. turvallisuusluokan tietojen kopiointiin hyväksymällä (akkreditoidulla) kopiokoneella. Jokainen kopio on numeroitava ja rekisteröitävä
- **Rekisteröitävä** ennen lähettämistä, vastaanottaessa ja hävitettäessä

- NATO SECRET –tietoaineisto **kuljetetaan** pääsääntöisesti sotilaskuriirilla, valtion kuriirilla tai diplomaattipostina
- tietoaineiston fyysistä kuljettamista tulisi välttää, jos tieto voidaan siirtää turvallisesti sähköisesti
- saa **kuljettaa** Nato-jäsenvaltion sisällä rakennelmien välillä henkilökohtaisesti kuriirivelvoittein edellyttäen, että:

    - aineisto on pakattu vähintään kahteen läpinäkymättömään kuoreen
    - pakkaus estää tiedon luvattoman ilmitulon
    - tietoaineiston turvallisuusluokka ja vastaanottaja käyvät ilmi vain pakkauksen sisimmästä kuoresta
    - ulompi kuori sisältää vastaanottajan tiedot (ei aineiston turvallisuusluokkaa) sekä mekanismin, jolla toimituksen toteutus voidaan dokumentoida
    - kuljetusvälinettä (salkku tms.) ei saa jättää missään oloissa vartioimatta ja sen tulee olla lukittu
    - lähetys tulee avata dokumentoidusti määränpäässä, tietoa ei saa avata kuljetuksen aikana
    - henkilökuriirilla tulee olla asianmukaisen tason PSC-todistus, hänen tulee perehtyä Naton turvallisuusmääräyksiin ja hänellä tulee olla kansallisten määräysten mukainen valtuutus sekä Naton säännösten mukainen henkilökuriiritodistus.

- saa **kuljettaa** Nato-valtioiden sekä kolmansien valtioiden välillä henkilökohtaisesti, mutta tämä edellyttää aina kansallisen turvallisuusviranomaisen erityisohjeistusta sekä myötävaikutusta

- **ei saa tuhota itse vaan hävitetään** kyseisen turvallisuusluokan vaatimusten mukaisesti vastuunalaisessa keskus-, ala- tai erillisrekisterissä.

4.3.4 COSMIC TOP SECRET

Korkeimman tason NATO turvallisuusluokitus. COSMIC TOP SECRET -luokan asiakirjojen laatiminen ja käsittely on harvinaista. Niiden käsittelyssä edellytetään NATO SECRET -luokan vaatimuksia, mutta käsittelijän henkilövalintaan liittyy erityistä harkintaa (käsittelyoikeudet ja turvallisuusselvitystason määrittely). Lisäksi kyseisen luokan asiakirjojen rekisteröinti ja hävittäminen poikkeavat alemmista turvallisuusluokista. Tietoa sähköisesti siirrettäessä salaustuotteelle edellytetään COSMIC TOP SECRET -luokan hyväksyntää Naton sotilaskomitealta. Tämän turvallisuusluokan tietojärjestelmästä ei saa olla suoria tai porrastettuja yhteyksiä suojaamattomiin verkkoihin.

- **Rekisteröitävä** ennen lähettämistä, vastaanottaessa ja hävitettäessä

- CTS-tietoa käsittelevien organisaatioiden on nimettävä **COSMIC-tiedon valvoja (CCO)**

- ei saa **kopioida** itse vaan lisäjakelua koskeva pyyntö tulee osoittaa asiakirjan laatijalle

- saa **lähettää** ainoastaan sotilaskuriiria, valtion kuriiria tai diplomaattipostia käyttäen
- kaupallisia kuriiripalveluita ei saa käyttää

- **ei saa tuhota itse, hävitetään** dokumentoidusti COSMIC-keskus- tai alarekisterissä kyseisen turvallisuusluokan vaatimusten mukaisesti.

5 MUIDEN VALTIOIDEN JA KANSAINVÄLISTEN JÄRJESTÖJEN TIETOAINEISTON KÄSITTELY

Kansainvälisissä turvallisuusluokiteltuja tietoja koskevissa sopimuksissa osapuolet sitoutuvat turvallisuusluokitellun tiedon vastavuoroiseen suojaamiseen: toisen osapuolen turvallisuusluokitellulle tiedolle annetaan samantasoinen suoja kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolle. Tätä varten sopimuksissa määritetään turvallisuusluokkien vastaavuudet ja yleiset periaatteet turvallisuusluokitellun tiedon vaihtamisesta. Sopimuksissa rajoitetaan turvallisuusluokitellun tiedon käyttö vain siihen tarkoitukseen, jota varten se on luovutettu. Sopimuksissa määritellään, missä tilanteissa sopimuspuolten lainsäädännön alaisuuteen kuuluvista yrityksistä ja yhteisöistä sekä henkilöistä laaditaan turvallisuusselvitys edellytyksenä turvallisuusluokiteltujen tietojen käsittelylle. Henkilöille myönnettävistä kansainvälisistä henkilöturvallisuusselvityksistä käytetään nimitystä PSC (*Personnel Security Clearance*). Vastaavasti yrityksille ja muille yhteisöille myönnettään yrityturvallisuustodistuksia FSC (*Facility Security Clearance*).

Linkki voimassa oleviin tietoturvallisuussopimuksiin

LYHENTEET

CAA	*Crypto Approval Authority,* Suomessa Liikenne- ja viestintäviraston NCSA-FI
CCO	*Cosmic Control Officer,* COSMIC-tiedon valvoja
DSA	*Designated Security Authority,* määrätty turvallisuusviranomainen
EUCI	*European Union Classified Information,* Euroopan unionin turvallisuusluokiteltu tieto
FSC	*Facility Security Clearance,* yritysturvallisuusselvitys
NCSA	*National Communication Security Authority,* kansallinen tietojärjestelmien ja tietoliikenteen tietoturvallisuudesta vastaava viranomainen
NOS	*NATO Office of Security,* Naton turvallisuustoimisto
NSA	*National Security Authority,* kansallinen turvallisuusviranomainen
PSC	*Personnel Security Clearance,* kansainvälinen henkilöturvallisuusselvitys
PSCC	*Personnel Security Clearance Certificate,* kansainvälinen henkilöturvallisuusselvitystodistus
PSCC	*Personnel Security Clearance Confirmation,* kansainvälinen henkilöturvallisuusvahvistus
SAA	*Security Accreditation Authority,* Suomessa Liikenne- ja viestintäviraston NCSA-FI
TEMPEST	*Temporary Emanations and Spurious Transmission,* termillä tarkoitetaan vaarantavaan hajasäteilyyn kohdistuvia tarkastuksia, tutkimuksia, kontrollointia, tiedustelu-uhkaa vastaan suoritettavia vastatoimia ja vaarantavaa hajasäteilyä vaimentavia (tukahduttavia) toimia

EU:ssa JA SEN JÄSENMAISSA KÄYTETTÄVIEN TURVALLISUUS-LUOKKIEN VASTAAVUUS

EU-TURVALLISUUS-LUOKKA	TRES SECRET UE / EU TOP SECRET	SECRET UE / EU SECRET	CONFIDENTIEL UE / EU CONFIDENTIAL	RESTREINT UE / EU RESTRICTED
Alankomaat	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Belgia	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	*ks. huomautus 1*
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Espanja	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Irlanti	Top Secret	Secret	Confidential	Restricted
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Itävalta	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Kreikka	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Kypros	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Kroatia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Liettua	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Malta ***ks. huomautus 2***	L-Ogħla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted

Portugali	Muito Secreto	Secreto	Confidencial	Reservado
Puola	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Ranska	Très Secret Défense / Très Secret	Secret Défense / Secret Défense	*Ks. Huomautus 3*	*ks. huomautus 4*
Romania	Strict secret de Importanță deosebită	Strict secret	Secret	Secret de serviciu
Ruotsi ***ks. huomautus 5***	HEMLIG/TOP SECRET KVALIFICERAT HEMLIG	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL KONFIDENTIELL	HEMLIG/RESTRICTED BEGRÄNSAT HEMLIG
Saksa	STRENG GEHEIM	GEHEIM	VS — VERTRAULICH (*ks. huomautus 6)*	VS — NUR FÜR DEN DIENSTGEBRAUCH
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Slovenia	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Suomi	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Tanska	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Tsekin tasavalta	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Unkari	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Viro	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud

HUOMAUTUKSET

1: Diffusion Restreinte / Beperkte Verspreiding ei ole Belgiassa turvaluokka. Belgia käsittelee ja suojaa RESTREINT UE/EU RESTRICTED -tiedot vähintään yhtä tiukasti kuin Euroopan unionin neuvoston turvallisuussäännöissä kuvatut vaatimukset ja menettelyt edellyttävät.

2: Maltassa voidaan käyttää sekä maltan- että englanninkielisiä merkintöjä.

3: Ranska on luopunut 1.7.2021 turvallisuusluokasta CONFIDENTIEL DEFENSE kansallisessa järjestelmässään. Ranska käsittelee ja suojaa CONFIDENTIEL UE/EU CONFIDENTIAL -tiedot vähintään yhtä tiukasti kuin Euroopan unionin neuvoston turvallisuussäännöissä kuvatut vaatimukset ja menettelyt edellyttävät.

4: Ranska ei käytä turvallisuusluokkaa RESTREINT kansallisessa järjestelmässään. Ranska käsittelee ja suojaa RESTREINT UE/EU RESTRICTED -tiedot vähintään yhtä tiukasti kuin Euroopan unionin neuvoston turvallisuussäännöissä kuvatut vaatimukset ja menettelyt edellyttävät.

5: Ruotsi: ylemmällä rivillä olevia turvaluokitusmerkintöjä käytetään puolustusvoimissa, ja alemmalla rivillä olevia merkintöjä käyttävät muut viranomaiset.

6: Saksa: VS = Verschlusssache.